

UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

DOCUMENT DYNAMICS, LLC,)
Plaintiff,) Civil Action No. 3:18-cv-00411-AVC
v.)
XEROX CORPORATION,) March 15, 2019
Defendant.)

)

**XEROX CORPORATION'S MEMORANDUM IN SUPPORT OF ITS
SUMMARY JUDGMENT MOTION OF INVALIDITY**

TABLE OF CONTENTS

I.	BACKGROUND.....	1
II.	ARGUMENT	3
	A. Summary Judgment Standard.....	3
	B. Claim 4 of the Patent-in-Suit Is Invalid	4
	1. Patent Ineligible Subject Matter under Section 101.....	4
	i. Claim 4 Is Directed to an Abstract Idea.....	5
	ii. Other Elements of Claim 4 Merely Describe Common Functions and Components Not Invented by Document Dynamics	7
	2. Anticipation under Section 102	12
	3. Obviousness under Section 103	18
	i. Caffary and Sabbagh.....	19
	ii. DPServer and Caffary	25
	iii. Coons and Shenoy	30
	iv. Secondary Factors.....	37
	3. Indefiniteness under Section 112	39
	i. “Assessing”	39
	ii. “Periodically”	40
III.	CONCLUSION.....	40

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Alice Corporation Pty. Ltd. v. CLS Bank International</i> , 573 U.S. 208 (2014)	4, 5, 7, 9-11
<i>Anderson v. Liberty Lobby, Inc.</i> , 477 U.S. 242 (1986)	3
<i>Apple Computer, Inc. v. Articulate Systems, Inc.</i> , 234 F.3d 14 (Fed. Cir. 2000)	12
<i>Apple, Inc. v. Ameranth, Inc.</i> , 842 F.3d 1229 (Fed. Cir. 2016).....	7
<i>Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.</i> , 796 F.2d 443 (Fed. Cir. 1986), <i>cert. denied</i> , 484 U.S. 823 (1987)	38
<i>In re Chu</i> , 66 F.3d 292 (Fed. Cir. 1995)	3
<i>Dann v. Johnston</i> , 425 U.S. 219 (1976)	37
<i>Easyweb Innovations, LLC v. Twitter, Inc.</i> , No. 11CV4550JFBSIL, 2016 WL 1253674 (E.D.N.Y. Mar. 30, 2016), <i>aff'd</i> , 689 F. App'x 969 (Fed. Cir. 2017).....	10
<i>Electric Power Group, LLC v. Alstom S.A.</i> , 830 F.3d 1350 (Fed. Cir. 2016).....	5, 7
<i>FairWarning IP, LLC v. Iatric Sys., Inc.</i> , 839 F.3d 1089 (Fed. Cir. 2016).....	5
<i>Graham v. John Deere Co.</i> , 383 U.S. 1 (1966)	37
<i>Intellectual Ventures I LLC v. Symantec Corp.</i> , 838 F.3d 1307 (Fed. Cir. 2016).....	5
<i>Interval Licensing LLC v. AOL, Inc.</i> , 766 F.3d 1364 (Fed. Cir. 2014).....	39

<i>Jacobs Vehicle Systems, Inc. v. Pacific Diesel Brake Co.,</i> 424 F. Supp. 2d 388 (D. Conn. 2006)	4
<i>Johnson Electric Industrial Manufacturing, Ltd. v. Ametek, Inc.,</i> 850 F. Supp. 2d 342 (D. Conn. 2006)	4
<i>KSR International Co. v. Teleflex Inc.,</i> 550 U.S. 398 (2007)	18, 25, 30, 37
<i>Mayo Collaborative Services v. Prometheus Laboratories, Inc.,</i> 566 U.S. 66 (2012)	11
<i>Mortgage Grader, Inc. v. First Choice Loan Services Inc.,</i> 811 F.3d 1314 (Fed. Cir. 2016).....	8
<i>Nautilus, Inc. v. Biosig Instruments, Inc.,</i> 572 U.S. 898 (2014)	39
<i>Noah Systems, Inc. v. Intuit Inc.,</i> 675 F.3d 1302 (Fed. Cir. 2012).....	39
<i>Perfect Web Technologies, Inc. v. InfoUSA, Inc.,</i> 587 F.3d 1324 (Fed. Cir. 2009).....	25
<i>Santarus, Inc. v. Par Pharm., Inc.,</i> 694 F.3d 1344 (Fed. Cir. 2012).....	3
<i>Smart Systems Innovations, LLC v. Chicago Transit Authority,</i> 873 F.3d 1364 (Fed. Cir. 2017).....	5
<i>Smithkline Beecham Corp. v. Apotex Corp.,</i> 403 F.3d 1331 (Fed. Cir. 2005).....	4
<i>Synopsys, Inc. v. Mentor Graphics Corp.,</i> 839 F.3d 1138 (Fed. Cir. 2016).....	5
<i>Ultramercial, Inc. v. Hulu, LLC,</i> 772 F.3d 709 (Fed. Cir. 2014).....	10
<i>Waldemar Link v. Osteonics Corp.,</i> 32 F.3d 556 (Fed. Cir. 1994)	2
<i>Zenith Electronics Corp. v. PDI Communication Systems, Inc.,</i> 522 F.3d 1348 (Fed. Cir. 2008).....	12
Statutes	
35 U.S.C. § 101.....	4, 7, 9, 12

35 U.S.C. § 102.....	4, 12, 18
35 U.S.C. § 103.....	4, 18
35 U.S.C. § 112.....	4, 39
35 U.S.C. § 120.....	2

Rules

Fed. R. Civ. P. 56(a).....	3
D. Conn. L. Civ. R. 56(a)1	1

Other Authorities

MPEP § 608.04(a).....	2
MPEP § 2159.....	12

Defendant Xerox Corporation respectfully submits this memorandum of law in support of its motion for summary judgment on the basis of invalidity of U.S. Patent No. 7,872,772.

I. BACKGROUND

Xerox Corporation (“Xerox”) is a global leader in business communications and presentation. Among other areas, Xerox has served the printing and copying needs of numerous companies via its managed print services since at least 1997, with various hardware and software configurations. Plaintiff Document Dynamics, LLC (“Document Dynamics”) commenced this patent infringement action on March 8, 2018. Document Dynamics asserts only Claim 4 of U.S. Patent No. 7,872,772, titled “Network Printing Tracking System,” issued on January 18, 2011. (Xerox’s Local Rule 56(a)1 Statement of Undisputed Material Facts (“SOF”) ¶ 1.)

Document Dynamics’ expert claims that:

The invention of the ‘772 provides for software to be wrapped around, or appended to, existing operating-system-level print drivers, for example on a print server or on a user workstation, in order to provide the ability to capture full details regarding the print transaction, by virtue of executing on the originating computer or the print server computer itself.

(Declaration of Elizabeth A. Alquist (“Alquist Decl.”) Ex. B (“Wedock Report”) ¶ 24; SOF ¶ 3.) In fact, Claim 4 recites:

A method for managing network printers in a network including a print server having at least one existing print driver, a plurality of client terminals, and at least one printer, comprising the steps of:

appending printer management agent software to the existing print driver on said print server for monitoring document, user and device metrics, inclusive of origination, generation, acquisition and destination metrics, to and from said at least one printer;

capturing said document, user and device metrics by said printer management agent software each time a print job is printed to said at least one printer; storing said captured document, user and device metrics in an encrypted file locally;

periodically writing said encrypted document, user and device metrics from said local file to a central data store; [and]

accessing said central data store and assessing said document, user and device metrics.

(Alquist Decl. Ex. A (“772 Patent”) Claim 4.) In short, the ’772 Patent concerns a method of attaching reporting (agent) software to a print driver running on a networked computer in order to track usage information for a printer on the same network. ’772 Patent col. 3 l. 22; Wedock Report ¶ 36 (“The novelty of the claim is the attaching of print reporting software, or “agent” software, to the print driver.”). (*See also* SOF ¶ 5.)

The ’772 Patent was filed on March 12, 2007, as a continuation-in-part of U.S. Patent No. 7,190,478, filed on May 29, 2002. (SOF ¶¶ 2, 7.) The ’478 Patent is directed to a system that similarly tracks print data, except that it requires substitute printer driver software replacing, instead of appending, the existing printer driver.¹ (Alquist Decl. Ex. D (“478 Patent”) Abstract.) Because the ’478 Patent does not disclose appending or supplementing print management software onto a print driver, Claim 4 is directed to “new matter”² and is not a continuation of the parent under 35 U.S.C. § 120. (SOF ¶¶ 9–11.) *See Waldemar Link v. Osteonics Corp.*, 32 F.3d 556, 558 (Fed. Cir. 1994) (“A CIP application can be entitled to different priority dates for different claims. Claims containing any matter introduced in the CIP are accorded the filing date of the CIP application. However, matter disclosed in the parent application is entitled to the

¹ For reference, Claim 1 of the ’478 Patent recites: “A system for outsourcing network printer requirements, comprising: . . . assessment software installed on the local area network and adapted to distribute and install Client PC software on each connected client PC, each Client PC software installation in turn replacing default printer driver software with substitute printer driver software that duplicates the function of the default printer driver software and additionally invisibly monitors print traffic data on said Client PC and captures print traffic data inclusive of UserLogon and all print related data for each print job for use in an assessment”

² *See* Manual of Patent Examining Procedure (“MPEP”) § 608.04(a) (“Matter not present on the filing date of the application in the specification, claims, or drawings that is added after the application filing is usually new matter.”).

benefit of the filing date of the parent application.”). Therefore, the priority date for Claim 4 of the ’772 Patent is March 12, 2007.³ (SOF ¶ 12.)

Document Dynamics recognizes this distinction between the ’478 Patent and the ’772 Patent in its expert report. More specifically, Document Dynamics’ expert states: “The invention of the ’772 Patent provides for software to be wrapped around, or appended to, existing operating-system-level print drivers, for example on a print server or on a user workstation in order to provide the ability to capture full details regarding the print transaction, by virtue of executing on the originating computer or the print server computer itself.” Weadock Report ¶ 24. (SOF ¶ 4.) Mr. Weadock additionally states that “appending printer management agent software to the existing print driver” must mean that the printer management agent software “supplements” the existing print driver. Weadock Report ¶ 26 (“The Xerox ‘XPA’ software (Xerox Print Agent) appends (in the sense of ‘supplements’) existing printing software, including a printer driver, on print servers and on workstations . . .”).) (SOF ¶ 6.) Accordingly, for the purpose of this motion only, it is assumed that “appending” in Claim 4 means “to supplement.”

II. ARGUMENT

A. Summary Judgment Standard

Summary judgment is appropriate when the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a). Initially, the burden rests on the moving party to establish the absence of any genuine issue of material fact. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242,

³ Again, Claim 4 cannot claim the priority date of the ’478 Patent, which does not disclose all of its claimed subject matter, e.g., “appending.” (SOF ¶ 9.) Where a claim of a continuation-in-part is not fully disclosed in the earlier filed patent, it cannot claim priority of the earlier patent. “Due to breaks in the chain of priority, [plaintiff] is unable to claim an early enough priority date to preclude use of Dr. Phillips’s own [earlier] patent as prior art for some of the asserted claims.” *Santarus, Inc. v. Par Pharm., Inc.*, 694 F.3d 1344, 1352 (Fed. Cir. 2012); *see also In re Chu*, 66 F.3d 292 (Fed. Cir. 1995).

252 (1986). Once this burden has been satisfied, however, the burden shifts to the non-moving party to “go beyond the pleadings to identify specific material facts that are in dispute.” *Jacobs Vehicle Sys. v. Pac. Diesel Brake Co.*, 424 F. Supp. 2d 388, 291 (D. Conn. 2006). The non-moving party must do more than raise some metaphysical doubt, but rather must “set forth specific facts showing that there is a genuine issue for trial.” *Johnson Elec. Indus. Mfg., Ltd. v. Ametek, Inc.*, 850 F. Supp. 2d 342, 345 (D. Conn. 2006). If the evidence brought forward by the nonmoving party is insufficient to return a jury verdict in its favor, summary judgment may be granted. *Johnson Elec. Indus. Mfg.*, 850 F. Supp. 2d at 345 (citing *Anderson*, 477 U.S. at 248).

B. Claim 4 of the '772 Patent Is Invalid

Claim 4 of the '772 Patent is invalid under 35 U.S.C. §§ 101 (ineligible subject matter), 102 (anticipation), 103 (obviousness), and 112 (indefiniteness) for at least the following reasons.⁴ Xerox respectfully requests that the Court find Claim 4 invalid as a matter of law, not only to dispose of the disputes between the parties but also for the public good. *See Smithkline Beecham Corp. v. Apotex Corp.*, 403 F.3d 1331, 1354 (Fed. Cir. 2005) (noting “a significant public policy interest in removing invalid patents from the public arena”).

1. Patent Ineligible Subject Matter under Section 101

The '772 Patent is invalid because it fails to claim patent-eligible subject matter. Under 35 U.S.C. § 101, only “new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof” may be patented. Both abstract ideas and well-known activities implemented via generic computer components and functions are not patent-eligible. *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 222 (2014). Claim 4 merely

⁴ 35 U.S.C. §§ 102 and 103 under the America Invents Act (“AIA”) apply to any patent application that contains or contained at any time a claim to a claimed invention that has an effective filing date that is on or after March 16, 2013. As the application leading to the '772 Patent was filed on March 12, 2007, the pre-AIA 35 U.S.C. §§ 102 and 103 apply.

recites the abstract idea of tracking print jobs using generic computers instead of pen and paper. Courts may invalidate such claims as a matter of law by summary judgment. *Synopsys, Inc. v. Mentor Graphics Corp.*, 839 F.3d 1138, 1146 (Fed. Cir. 2016).

Under the Supreme Court's two step analysis, courts first "determine whether the claims at issue are directed to a patent-ineligible concept." *Alice*, 573 U.S. at 217. If, like here, it is, courts then "consider the elements of each claim both individually and as an ordered combination to determine whether the additional elements transform the nature of the claim into a patent-eligible application." *Id.* (internal quotation marks and citation omitted).

i. Claim 4 Is Directed to an Abstract Idea

Claim 4 is directed to a method of tracking printer usage information. Courts have found similar concepts relating to collecting, analyzing, and displaying information as ineligible for patent protection, such as screening and tracking emails, phone calls and banking information. *See, e.g., Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1314 (Fed. Cir. 2016) (invalidating claims directed to (i) methods of screening e-mails and other data files for unwanted content; (ii) methods of routing e-mail messages based on specified criteria; and (iii) using computer virus screening in a telephone network); *Smart Systems Innovations, LLC v. Chicago Transit Authority*, 873 F.3d 1364, 1372–73 (Fed. Cir. 2017) (claims directed to acquiring identification data from a bankcard, using the data to verify the bankcard's validity, and denying access to a transit system if the bankcard is invalid); *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1094–95 (Fed. Cir. 2016) (claims "directed to collecting and analyzing information to detect misuse and notifying a user when misuse is detected" were drawn to a patent-ineligible abstract idea); *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353–54 (Fed. Cir. 2016) (collecting cases invalidating claims directed to an abstract idea because "[t]he

advance they purport to make is a process of gathering and analyzing information of a specified content, then displaying the results, and not any particular assertedly inventive technology for performing those functions”).

Here, Claim 4 merely recites the concept of tracking printer usage information that is, who printed what and at which printer.

A method for managing network printers in a network including a print server having at least one existing print driver, a plurality of client terminals, and at least one printer, comprising the steps of:

appending printer management agent software to the existing print driver on said print server for monitoring document, user and device metrics, inclusive of origination, generation, acquisition and destination metrics, to and from said at least one printer;

capturing said document, user and device metrics by said printer management agent software each time a print job is printed to said at least one printer; storing said captured document, user and device metrics in an encrypted file locally;

periodically writing said encrypted document, user and device metrics from said local file to a central data store; [and]

accessing said central data store and assessing said document, user and device metrics.

'772 Patent Claim 4 (emphases added). Indeed, the '772 Patent describes the putative invention as a “software system and method of monitoring and tracking print transaction event history for a pipeline users, devices, applications and documents in a network environment.” *Id.* Abstract.

The specification further describes that such activity was historically done manually. “The management of client printer configurations has traditionally been a manual process and all printer drivers must be manually installed and network connections manually established.” *Id.* col. 2 ll. 1-4. Moreover, Document Dynamics’ discovery requests and Motion to Compel contend that “Accused Instrumentality” includes at least all “products, systems or methods that

are capable of, or advertised or marketed as being capable of monitoring and tracking print transaction events for users, devices, applications, and documents through the use of hardware, software or any combination thereof.” (Dkt. No. 33-2 at 1–2.)

Assuming, *arguendo*, that Document Dynamics is correct about the purported scope of Claim 4, it necessarily follows that Claim 4 is directed to the abstract concept of tracking printer usage information. Indeed, Claim 4 does not specify *how* the printer usage information is monitored and captured, and therefore, improperly claims the resultant method. *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1244 (Fed. Cir. 2016) (“Generally, a claim that merely describes an effect or result dissociated from any method by which it is accomplished is not directed to patent-eligible subject matter.”) (citation omitted). Try as it might, Document Dynamics cannot under Section 101 claim the practice of tracking printer usage information as to preclude all means of doing so by any and all hardware and software—none of which it invented. *See Elec. Power Grp.*, 830 F.3d at 1356 (cautioning against claims “so result-focused, so functional, as to effectively cover any solution to an identified problem”). *See also Alice*, 573 U.S. at 216 (“We have described the concern that drives this exclusionary principle as one of pre-emption.”).

ii. Other Elements of Claim 4 Merely Describe Common Functions and Components Not Invented by Document Dynamics

The concept of tracking printer usage was not invented by Document Dynamics and cannot itself be patented. Furthermore, all other elements of Claim 4 are common functions and components that do not provide any inventive concept. Using generic computer components and functions to implement well-known activities does not render the claim patentable. *Alice*, 573 U.S. at 223. (“[T]he mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention”). Similarly, limiting the claim to a particular

technological field does not render the claim patentable. *Id.* (citing *Bilski v. Kappos*, 561 U.S. 593, 610–611 (2010)).

Here, the elements of Claim 4, separately or in combination, do not provide any inventive concept. Instead, Claim 4 is directed to the well-known practice of tracking printer usage information with nothing but common components and functions. Each element is discussed, below, *seriatim*.

The limiting preamble of Claim 4 states: ***A method for managing network printers in a network including a print server having at least one existing print driver, a plurality of client terminals, and at least one printer, comprising the steps of.***

Network printers, a network, a print server, a print driver, client terminals, and a printer are each common components that Document Dynamics did not invent. The '772 Patent admits that connecting these components via a network were well known prior to the filing date of the application that issued as the '772 Patent as were methods for managing networked devices. “A primary goal of local area network (LAN) technology is to share all resources that are distributed across the network. Existing network software helps network administrators to accomplish this purpose.” '772 Patent col. 1 ll. 33-36. Furthermore, a print server is merely a personal computer, as noted in the '772 Patent as “server PC.” *Id.* col. 3 l. 15. Likewise, a printer driver on a print server or personal computer is a common computer component that Document Dynamics cannot and does not claim to have invented. Wedock Report ¶ 24 (“The invention of the '772 provides for software to be wrapped around, or appended to, existing operating-system-level print drivers, for example on a print server or on a user workstation . . .”). *See also Mortg. Grader, Inc. v. First Choice Loan Servs. Inc.*, 811 F.3d 1314, 1324–25 (Fed. Cir. 2016) (holding

that “generic computer components such as an ‘interface,’ ‘network,’ and ‘database’ . . . do not satisfy the inventive concept requirement”)

The first element of Claim 4 states: ***appending printer management agent software to the existing print driver on said print server for monitoring document, user and device metrics, inclusive of origination, generation, acquisition and destination metrics, to and from said at least one printer.***

Assuming for purposes of this motion only that “appending” is to “supplement” as suggested by Document Dynamics’ expert (SOF ¶ 6), appending one type of software to another was also common long before the time of the alleged invention. Applets, servlets and plug-ins are well known examples of software programs whose purpose is to supplement associated software programs. Indeed, having software to supplement another software component is a meaningless step, as generic as stating “add software to implement the well-known activity of tracking printer usage information.” Such a non-specific element does not provide “something more” required under Section 101. *See Alice*, 573 U.S. at 223 (“Thus, if a patent’s recitation of a computer amounts to a mere instruction to ‘implement’ an abstract idea ‘on . . . a computer,’ that addition cannot impart patent eligibility.”). Without any specific improvement to the manner of supplementing a print driver with the agent software, Document Dynamics cannot proclaim it is entitled to patent the common function of appending the print driver.

The second element of Claim 4 states: ***capturing said document, user and device metrics by said printer management agent software each time a print job is printed to said at least one printer.***

This element does nothing more than data gathering (i.e., counting). Capturing who printed what—by hand or computer software—is not inventive. *See Alice*, 573 U.S. at 225

(holding that electronic recordkeeping is “one of the most basic functions of a computer”). *See also Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 715 (Fed. Cir. 2014) (finding a step of “recording the transaction event to the activity log . . . including updating the total number of times” the event has occurred, as “routine, conventional activity”).

The third element of Claim 4 states: ***storing said captured document, user and device metrics in an encrypted file locally:***

Storing the captured information in an encrypted file is not inventive, as cryptology dates back to Egyptian times. Encrypting files and storing them dates back to the very first computers. Similarly, transmitting the encrypted file to a central location where data is stored is a common function unworthy of patent protection. *See Easyweb Innovations, LLC v. Twitter, Inc.*, No. 11CV4550JFBSIL, 2016 WL 1253674, at *28 (E.D.N.Y. Mar. 30, 2016), *aff'd*, 689 F. App'x 969 (Fed. Cir. 2017) (“Courts have previously found that patents involving the transformation and transmission of information in one form to another form constituted abstract ideas.”)

The fourth element of Claim 4 states: ***periodically writing said encrypted document, user and device metrics from said local file to a central data store:***

A “central data store” is also common. *See Alice*, 573 U.S. at 226 (“[W]hat petitioner characterizes as specific hardware . . . ‘data storage unit,’ for example . . . is purely functional and generic. Nearly every computer will include a . . . ‘data storage unit’ capable of performing the basic calculation, storage, and transmission functions required by the method claims. As a result, none of the hardware recited by the system claims offers a meaningful limitation beyond generally linking the use of the method to a particular technological environment, that is, implementation via computers.”).

The final element of Claim 4 states: ***accessing said central data store and assessing said document, user and device metrics.***

Finally, accessing or assessing⁵ the tracked information are insignificant activities that cannot be patented. *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 79 (2012) (“[T]he prohibition against patenting abstract ideas cannot be circumvented by . . . adding insignificant postsolution activity.”) (internal quotation marks and citation omitted). Similar to the “determining” step in *Mayo* that the Supreme Court found insignificant, accessing or assessing here are insignificant steps, presumably of looking at what has been gathered (without any more direction). Accordingly, the final step does not add any inventive concept.

Document Dynamics shows its concern in the Complaint that the '772 Patent covers ineligible subject-matter. The Complaint attempts to address the *Alice* issue, alleging that the “inventions of the '772 Patent resolve technical problems related to network printer management. For example, the inventions allow parties to monitor and track print transaction events for users, devices, applications, and documents through the use of print agent software.” (Complaint ¶ 17.) The invention of Claim 4 of the '772 Patent, however, does not address any technical problem of network printer management. Claim 4, as discussed above, merely provides an accounting function to an already existing printer management system.

Document Dynamics’ statements regarding “problems specifically arising in the realm of printer management technology” do not render Claim 4 patent eligible. (Complaint ¶ 18.) “Stating an abstract idea while adding the words ‘apply it’ is not enough for patent eligibility. Nor is limiting the use of an abstract idea ‘to a particular technological environment.’” *Alice*, 573 U.S. at 223. Document Dynamics’ purported invention does not achieve any improved

⁵ The Patent does not even make clear what assessing means. *See, infra*, § II(B)(4)(ii). It is hard to think of anything more generic than “accessing or assessing.”

technological result; instead, it attempts to capture the idea of tracking print jobs using generic hardware and software instead of a pen and paper, which is precisely what *Alice* prohibits.

Here, there are no additional features, separately or as a combination, beyond well-known, generic components such as a printer driver and data store, performing their common functions. The elements therefore do not convert the abstract idea of tracking printer usage information into a patent-eligible claim, because they do not meaningfully distinguish the abstract idea over the patent ineligible claim. Thus, Xerox respectfully request that the Court find Claim 4 invalid under Section 101.

2. Anticipation under Section 102

Claim 4 is anticipated by at least U.S. Patent Application No. 2005/0259289. (Alquist Decl. Ex. C (“Ferlitsch”).) Anticipation is a question of fact that may be resolved on summary judgment if no reasonable jury could find that the patent is not anticipated by the prior art. *Zenith Elecs. Corp. v. PDI Communication Systems, Inc.*, 522 F.3d 1348, 1356–57 (Fed. Cir. 2008). If the prior art reference discloses each and every element of the claimed invention, the court must find the claim invalid as anticipated. *Apple Computer, Inc. v. Articulate Sys., Inc.*, 234 F.3d 14, 20 (Fed. Cir. 2000).

Ferlitsch is a patent application filed on May 10, 2004 and published on November 24, 2005. (SOF ¶ 14.) As Ferlitsch was published in this country more than one year prior to March 12, 2007, the date of application of the ’772 Patent, Ferlitsch is prior art under pre-AIA Section 102(b).⁶ (SOF ¶ 15.) Ferlitsch is titled “Print Driver Job Fingerprinting” and discloses a print job generation system that adds a “fingerprint” image, that is user information, to a document.

⁶ Again, as the application for the ’772 Patent was filed prior to enactment of the AIA, pre-AIA 35 U.S.C. § 102(b) governs. See MPEP § 2159 (applying pre-AIA provisions on applications filed before March 16, 2013).

The fingerprinting process may take place at the client computing device or print server for printers that are “locally, network, or remotely connected.” Ferlitsch ¶¶ 0011–12; *see also id.*

Figure 4B. The print job generation system may be embedded in “a client computing device, a printer, or a print server.” *Id.* ¶ 0038. Accordingly, Ferlitsch discloses managing network printers in a network that includes a print server having at least one existing print driver, a plurality of client terminals, and at least one printer.

Ferlitsch, in FIG. 2A, depicts the introduction of fingerprint information at the print source. The print subsystem, at the source initiating the print job, adds the fingerprint to the print data. For example, the fingerprint may be added by a printer driver. *Id.* ¶ 0032. This Fingerprinting Print Driver is added to the system prior to the existing print driver (“print processor”) as shown in Fig. 2A. The print job generation system gathers as input, fingerprint information, such as “job ownership/origination,⁷ host, target printer,⁸ routing, job assembly, job scheduling,⁹ metadata, or job content information.” *Id.* ¶ 0014 (emphases added); *see also id.* ¶¶ 0061–95. Ferlitsch also discloses automatically gathering such fingerprint information from an electronically-formatted document. *Id.* ¶ 0045. Therefore, Ferlitsch discloses “appending printer management agent software to the existing print driver on said print server for monitoring document, user and device metrics, inclusive of origination, generation, acquisition and destination metrics, to and from said at least one printer.” *See also id.* ¶¶ 0054, 60 (“Print job

⁷ “Job ownership/origination fingerprint information includes user name, biometric data, and a digital signature associated with the source of the electronically formatted document.” Ferlitsch ¶ 0043.

⁸ “Target printer fingerprint information includes printer name, printer model name, printer serial number, printer network address.” *Id.* ¶ 0044.

⁹ “Job scheduling fingerprint information includes job name, job ID, job submission time and date, and job size. Job assembly fingerprint information includes the number of pages/sheets, sheet assembly (duplex, n-up, booklet, tri-fold), finishing (stapling, folding, hole-punching, cutting, trimming), collation (copies, face-up, color separation), rendering (color, dpi, resolution), and consumables (paper stock and ink).” *Id.* ¶ 0043.

information may be collected through a variety of means, but not limited to: . . . Monitoring the Print Job.”).

Ferlitsch discloses that the print job generation system adds the fingerprint image either prior to rendering the print job or while rendering the print job. *Id.* ¶ 0046. In addition, Ferlitsch discloses that “[d]uring the rendering or journaling process, the printer driver collects information on the print job origin, print destination device and intermediate destination devices, such as a print server, and records some or all of the information as a fingerprint, by any means, into a pre-RIP or journaled print job. . . . The fingerprint may also be further secured by encryption and access control mechanisms.” *Id.* ¶ 0053. As a result, Ferlitsch discloses “capturing said document, user and device metrics by said printer management agent software each time a print job is printed to said at least one printer” and “storing said captured document, user and device metrics in an encrypted file locally.”

Ferlitsch also discloses that the encrypted fingerprint information is sent to a central data store (i.e., a spooler). “Generally, the output from the print driver, for example a spool file, is spooled to a spooler.” *Id.* ¶ 0052. Accordingly, Ferlitsch discloses “periodically writing said encrypted document, user and device metrics from said local file to a central data store.” Ferlitsch additionally discloses that the fingerprinted print job, with “job ownership/origination, host, target printer, routing, job assembly, job scheduling, metadata, or job content information” is subsequently printed at a printing device. *Id.* “The rendering system 324 (i.e., printer, scanner, fax, http server, document server, email server, or print job converter system) may accept the fingerprinted print job with the encrypted information image and supply a rendered print job with the decrypted fingerprint image on line 326. For example, a printer may decrypt the information and superimpose the information in decrypted form as a watermark overlying a

printed document.” *Id.* ¶ 0049. As the fingerprint information sent to a printer is accessed for decryption and printed for further analysis, Ferlitsch discloses “accessing said central data store and assessing said document, user and device metrics.”

In summary, Ferlitsch discloses each and every element of Claim 4 of the ’772 Patent as summarized in the claim chart below:

Claim 4 of the ’772 Patent	Ferlitsch (U.S. Application No. 2005/0259289)
A method for managing network printers in a network including a print server having at least one existing print driver, a plurality of client terminals, and at least one printer, comprising the steps of:	<p>Ferlitsch provides a method for managing network printers in a network including a print server having at least one existing print driver, a plurality of client terminals, and at least one printer. Ferlitsch discloses that its print job generation system on the client computing device and/or server computing device adds a fingerprint image to print jobs, including documents. “In this aspect, the fingerprinting print driver can be on the client computing device and/or server computing device, in the case of a journaled print job, such as EMF, spooled to a network printer.” Ferlitsch ¶ 0096.</p>

Fig. 4B

```

graph TD
    subgraph PS [PRINT SERVER]
        direction TB
        PQ((Print Queue)) -- "Printing Instructions (e.g., EMF)" --> FPD((Fingerprinting Printer Driver))
        OS((OS)) -- "Host Info" --> FPD
        FPD -- "Query/Response Printer Information" --> CI[CLIENT]
        FPD -- "Print Job + Pre-RIP Fingerprint" --> Spooler((Spooler))
        FPD -- "Print Job + Pre-RIP Fingerprint" --> PP((Print Processor))
        FPD -- "Print Job + Pre-RIP Fingerprint" --> PM((Port Manager))
        Spooler -- "Print Job + Pre-RIP Fingerprint" --> PRINTER[PRINTER]
        PP -- "Print Job + Pre-RIP Fingerprint" --> PRINTER
        PM -- "Print Job + Fingerprint" --> PRINTER
    end
    PRINTER -- "Print Job + Fingerprint" --> CI
    CI -- "Query/Response Client Information" --> PS

```

<p>appending printer management agent software to the existing print driver on said print server for monitoring document, user and device metrics, inclusive of origination, generation, acquisition and destination metrics, to and from said at least one printer;</p>	<p>Ferlitsch discloses appending printer management agent software (print job generation system) to the existing print driver on the print server for monitoring document, user and device metrics, inclusive of origination, generation, acquisition and destination metrics, (fingerprint information) to and from said at least one printer. The print job generation system may be a print driver or additional software supplementary to the driver. “FIG. 2A depicts the introduction of fingerprint information at the print source. The print subsystem, at the source initiating the print job, adds the fingerprint to the print data. For example, the fingerprint may be added by a printer driver, as described in pending application WO0174053.” Ferlitsch ¶ 0032. This Fingerprinting Print Driver is added to the system prior to the existing print driver (“print processor”) as shown in Fig. 2A.</p> <p style="text-align: center;"><i>Fig. 2A</i></p> <pre> graph TD Application((Application)) -- "Printing Instructions" --> FPD((Fingerprinting Printer Driver)) FPD -- "RIP + Fingerprint" --> Spooler((Spooler)) Spooler -- "RIP + Fingerprint" --> PrintProcessor((Print Processor)) PrintProcessor -- "RIP + Fingerprint" --> PortManager((Port Manager)) PortManager -- "RIP + Fingerprint" --> PRINTER[PRINTER] subgraph CLIENT [CLIENT] Application FPD Spooler PrintProcessor PortManager end </pre> <p>Collected fingerprint information includes document, user, and device metrics, including origination, generation, acquisition, and destination metrics, such as job name, printer name, and user name. “The print job generation system 302 accepts fingerprint information on line 306 such as job ownership/origination, host, target printer, routing, job assembly, job scheduling, metadata, and/or job content information. Job ownership/origination fingerprint information includes user name, biometric data, and a digital signature associated with the source of the</p>
--	---

	<p>electronically formatted document. Job scheduling fingerprint information includes job name, job ID, job submission time and date, and job size. Job assembly fingerprint information includes the number of pages/sheets, sheet assembly (duplex, n-up, booklet, tri-fold), finishing (stapling, folding, hole-punching, cutting, trimming), collation (copies, face-up, color separation), rendering (color, dpi, resolution), and consumables (paper stock and ink). Routing fingerprint information includes print server name, print server queue, print server network address, port name, and print provider. Host fingerprint information includes host name, host machine address (MAC), and host network address, such as an IP address. Target printer fingerprint information includes printer name, printer model name, printer serial number, printer network address. Metadata fingerprint information includes access control and anti-copy protection information. That is, information concerning who has access to see, print, or distribute the print job. In another aspect, the print job generation system 302 analyzes content information from the electronically formatted document, and generates a fingerprint image in response to the content information analysis.” Ferlitsch ¶ 0043-45.</p>
<p>capturing said document, user and device metrics by said printer management agent software each time a print job is printed to said at least one printer;</p>	<p>Ferlitsch discloses capturing the document, user, and device metrics by the printer management agent software each time a print job is printed. The print job generation system collects the fingerprint information either prior to rendering the print job or while rendering the print job. “Generally, the print job generation system 302 adds the fingerprint image to the print job either prior to rendering the print job, or while rendering the print job. In some aspects of the system, the print job generation system 302 generates and spools journaled data to the print subsystem 312. Subsequently, the print job generation system 302 despools the journaled data and adds the fingerprint image.” Ferlitsch ¶ 0046.</p>
<p>storing said captured document, user and device metrics in an encrypted file locally;</p>	<p>Ferlitsch discloses storing the captured document, user, and device metrics in an encrypted file locally. “During the rendering or journaling process, the printer driver collects information on the print job origin, print destination device and intermediate destination devices, such as a print server, and records some or all of the information as a fingerprint, by any means, into a pre-RIP or journaled print job. . . . The fingerprint may also be further secured by encryption and access control mechanisms.” Ferlitsch ¶ 0053.</p>
<p>periodically writing said encrypted</p>	<p>Ferlitsch discloses periodically writing the encrypted file containing the document, user, and device metrics from the local file to a central data</p>

document, user and device metrics from said local file to a central data store;	store. “Generally, the output from the print driver, for example a spool file, is spooled to a spooler.” Ferlitsch ¶ 0052; Fig. 4B.
accessing said central data store and assessing said document, user and device metrics.	Ferlitsch discloses accessing the central data store and assessing the document, user, and device metrics. The fingerprint information sent to a printer, for example, is accessed for decryption and assessed by overlying in printed document. “The rendering system 324 (i.e., printer, scanner, fax, http server, document server, email server, or print job converter system) may accept the fingerprinted print job with the encrypted information image and supply a rendered print job with the decrypted fingerprint image on line 326. For example, a printer may decrypt the information and superimpose the information in decrypted form as a watermark overlying a printed document.” Ferlitsch ¶ 0049.

As Ferlitsch discloses each and every element of Claim 4 of the '772 Patent, Xerox respectfully requests that the Court invalidate Claim 4 as anticipated under pre-AIA Section 102(b).

3. Obviousness under Section 103

Claim 4 is additionally invalid as it is rendered obvious in combination of prior art under pre-AIA Section 103(a).¹⁰ Obviousness is a question of law. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 427 (2007). Summary judgment of obviousness is appropriate where the difference between the patent claim and the prior art are such that the claim would have been obvious to a person of ordinary skill in the art at the time of the claimed invention. *Id.* at 406 (listing four relevant factors of (1) the scope and content of the prior art; (2) the level of ordinary skill in the

¹⁰ “A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.”

pertinent art;¹¹ (3) the differences, if any, between the prior art and the claims at issue; and (4) the impact of any secondary considerations on the obviousness inquiry). The following combinations of prior art references render Claim 4 of the '772 Patent obvious.¹²

i. Caffary and Sabbagh

U.S. Patent Application No. 2005/0259289 was filed on May 29, 2002 and published on December 4, 2003. (Alquist Decl. Ex. E (“Caffary”); SOF ¶ 8.) U.S. Patent Application No. 2002/0101600 was filed on January 29, 2001 and published on August 1, 2002.¹³ (Alquist Decl. Ex. F (“Sabbagh”); SOF ¶ 16.) As both applications were published in this country more than one year prior to March 12, 2007, the date of application for the '772 Patent, they are prior art to Claim 4 of the '772 Patent under Pre-AIA Section 102(b). (SOF ¶¶ 13, 17.) The combination of Caffary and Sabbagh renders Claim 4 obvious, as a person of ordinary skill would have been motivated to combine the two references with reasonable expectation of success, the result of which discloses each and every element of Claim 4.

Caffary concerns a method “implemented on a local area network including a server PC, a plurality of connected client PCs, and a plurality of printers each networked through a secure

¹¹ For purposes of this motion only, Xerox does not contest Document Dynamics’ level of skill for the '772 Patent—“a person with a good working knowledge of software development; an understanding of the software mechanisms for local and network printing in office networks, and familiarity with methods for monitoring print activities in such networks. The person would have gained this knowledge through an undergraduate Bachelor of Science degree in Computer Science, or other technical degree incorporating computer science courseware, and three to five years of experience working in the field of software development and/or systems integration. Additional education or experience may serve as a substitute for these requirements.” Wedock Report ¶ 21. (SOF ¶ 25.)

¹² Additional combinations of prior art references render Claim 4 obvious. For example, the references discussed below can be combined with Ferlitsch discussed *supra* to render Claim 4 obvious. Xerox expressly reserves its rights to assert additional combinations of prior art references as bases for invalidity, including but not limited to the 26 combinations it charted in response to Plaintiff’s discovery requests.

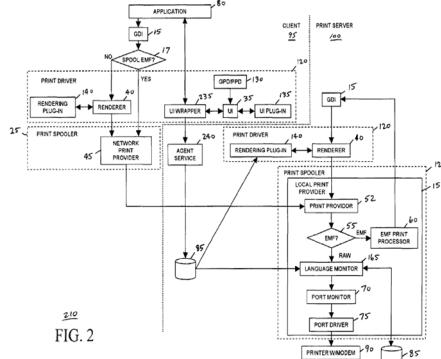
¹³ Caffary issued as U.S. Patent No. 7,190,478 on March 13, 2007. Sabbagh was assigned to Xerox on January 24, 2001 and issued as U.S. Patent No. 7,471,405 on December 30, 2008.

network connection device that communicates only with Secure Print Servers.” Caffary Abstract. Caffary discloses “track[ing] and record[ing] all print job related data, each time a print job is printed” *Id.* ¶ 0068. Specifically, Caffary tracks and records document, user, and device related data such as “PrinterName, MachineName, DriverName, Location, UserLogon, MachineName, DocumentName, DataType, Copies, FileSize, Submitted, PagesPrinted.” *Id.* ¶¶ 0072–83 (emphasized added). Caffary discloses that the captured data is encrypted and transmitted to a database on a variable time schedule, such as every 11 seconds to every 11 minutes. *Id.* ¶¶ 0068, 66. Caffary discloses that the data is “accessible” and reviewed using “the Assessment Database PC Software.” *Id.* ¶¶ 0054, 95 (emphasis added). Caffary discloses that its Client PC Software installs temporary drivers that duplicate the existing device drivers. *Id.* ¶ 0068. In sum, Caffary discloses every element of Claim 4, except the new matter disclosed for the first time in the ’772 Patent, namely “appending printer management agent software to the existing print driver.” Instead, Caffary discloses “replacing default printer driver software with substitute printer driver software.” *Id.* Claim 1.

Sabbagh discloses an operating system printing architecture that permits print job attributes from a client to have a desired effect on a print server operating in a networked environment. Sabbagh Abstract. Notably, the operating system printing architecture disclosed in Sabbagh includes: 1) an augmented print driver for collecting certain print job attributes and for rendering the print job. *Id.* It also includes: 2) an augmented print spooler for processing the print job and for directing the print job to a target device, and 3) an agent service to enable print job attributes collected on the client when a print job is initiated to be used by the print server when the print job is processed. *Id.* The Sabbagh operating system printing architecture also permits print jobs to be sent to multiple recipients. The augmented print spooler creates multiple

copies of the print job when it is directed to multiple recipients, one copy for each recipient. Like Caffary, Sabbagh discloses a software module that “indexes the print job attributes to the print job.” *Id.* ¶ 0030. In particular, Sabbagh discloses a “User interface wrapper” that “augments a standard print driver within a standard operating system printing architecture by creating hooks and enabling additional functionality and enhancements to be defined and implemented beyond those in the standard user interface.” *Id.* ¶ 0022. Therefore, Sabbagh discloses Caffary’s sole missing element of “appending printer management agent software to the existing print driver,” and the two prior art references in combination disclose each and every element of Claim 4 of the ’772 Patent, as summarized in the chart below:

Claim 4 of the ’772 Patent	Caffary (U.S. Patent Application Publication No. 2005/0259289)	Sabbagh (U.S. Patent Application Publication No. 2002/0101600)
4. A method for managing network printers in a network including a print server having at least one existing print driver, a plurality of client terminals, and at least one printer, comprising the steps of:	Caffary discloses a method for managing network printers in a network including a print server having at least one existing print driver, a plurality of client terminals, and at least one printer. “The Client PC Software installs temporary software device drivers in the Windows printing sub-system on the PCS. These device drivers duplicate the function of the default Windows device drivers and are invisible to the Client PCs 60-1 . . . n, but in addition, track and record all print job related data, each time a print job is printed on a client PC 60-1 . . . n to a locally attached printer, or a server-attached printer, or to remote network printers communicating either by TCP/IP protocol or IPX/SPX protocol.” Caffary ¶ 0068.	
appending printer management	Caffary discloses monitoring document, user and device metrics, inclusive of origination, generation,	Sabbagh discloses appending printer management agent software (user interface wrapper) to the existing print

<p>agent software to the existing print driver on said print server for monitoring document, user and device metrics, inclusive of origination, generation, acquisition and destination metrics, to and from said at least one printer;</p>	<p>acquisition and destination metrics, to and from the printer. “The Client PC Software serves to invisibly monitor print traffic on that client and collect data for use in the assessment. Each time a print job is created on any Client PC 60-1 . . . n, the Client PC Software device driver intercepts the job instantaneously and temporarily stores the data in a file on the Client PC.” Caffary ¶ 0066.</p> <p>Caffary lists the monitored information in detail, including printer name, user logon, and document name. “At least the following data is sent by the Client PC software and stored in the Assessment Database: PrinterName, MachineName, DriverName, Location, UserLogon, MachineName, DocumentName, DataType, Copies, FileSize, Submitted, PagesPrinted. In addition, the following data may be captured Orientation, Paper Size, Paper Length, Paper Width, Scale, Print Quality, Yresolution, Color, Duplex, TTOption.” Caffary ¶¶ 0071–94.</p>	<p>driver on a print server. The user interface (“UI”) wrapper monitors print job attributes. “The UI wrapper 235 indexes the print job attributes to the print job and notifies the print server 100 of the pending print job. The agent service 240 on the print server 100 monitors the network for transmissions from the UI wrapper 235. Once the agent service 240 recognizes and acknowledges such a transmission is pending, the agent service 240 and the UI wrapper 235 negotiate transfer of the indexed print job attributes over the network. The agent service 240 stores the indexed print job attributes in temporary files on the storage device 85.” Sabbagh ¶ 0030.</p> <p>The user interface wrapper augments and supplements a standard print driver. “‘User interface wrapper’ refers to a software module that augments a standard print driver within a standard operating system printing architecture by creating hooks and enabling additional functionality and enhancements to be defined and implemented beyond those in the standard user interface.” Sabbagh at ¶ 0022.</p> 
<p>capturing said document, user and device metrics</p>	<p>Caffary discloses capturing the document, user, and device metrics each time a print job is printed to the printer. “Given proper installation as</p>	

<p>by said printer management agent software each time a print job is printed to said at least one printer;</p>	<p>per the above, all print jobs pass through the secure Print Servers and all print related data for each job is captured by the Print Job Tracking Software installed on the Secure Print Servers.” Caffary ¶ 0052.</p> <p>“The Client PC Software installs temporary software device drivers in the Windows printing sub-system on the PCS. These device drivers . . . track and record all print job related data, each time a print job is printed on a client PC 60-1 . . . n to a locally attached printer, or a server-attached printer, or to remote network printers communicating either by TCP/IP protocol or IPX/SPX protocol.” Caffary ¶ 0068.</p>	
<p>storing said captured document, user and device metrics in an encrypted file locally;</p>	<p>Caffary discloses storing the captured document, user, and devices metrics in an encrypted file locally. “The Client PC Software installs temporary software device drivers in the Windows printing sub-system on the PCS. These device drivers . . . track and record all print job related data The Client PC Software then encrypts this data and sends it using TCP/IP.” Caffary ¶ 0068.</p> <p>“Periodically, the Client PC Software moves this temporary file in an encrypted file in the Client PC Software installation directory named during the installation of the software. Encryption is essential to prevent tampering and/or unauthorized use of the data.” Caffary ¶ 0066.</p>	
<p>periodically writing said encrypted document, user and</p>	<p>Caffary discloses periodically writing the encrypted document, user, and device metrics from the local file to a central data store (assessment database). “The Client PC Software</p>	

device metrics from said local file to a central data store;	then transmits the encrypted data to the Assessment Database Administrative PC on a variable time schedule that varies in accordance with print activity and is intended to minimize network traffic. For instance, if there is no print activity, then the Client PC Software reporting schedule will slow down to a minimum frequency. It has been found that a ranges of from every 11 seconds to every 11 minutes is suitable.” Caffary ¶ 0066.	
accessing said central data store and assessing said document, user and device metrics.	Caffary discloses accessing the central data store and assessing the document, user, and device metrics. “The data is then accessible on a secure basis by each dealer, for billing and operational purposes” Caffary ¶ 0054. “Given the foregoing data collected from all the Client PCs, a user can logon to the Assessment Database PC Software and generate a variety of reports.” Caffary ¶ 0095.	

A person of ordinary skill would have been motivated to combine Caffary and Sabbagh, as they both concern the same technical field— using enhanced print drivers to collect, track, and index print attributes. As a result, substituting Caffary’s replacement print drivers with Sabbagh’s User interface wrapper that augments a standard print driver would have been obvious to try in order to “manag[e] the diverse operating systems of the client computers, and the numerous printer drivers required for each different type of printer and for each different operating system, and the management problems created by a mixture of end-user attached and network attached printers.” Caffary ¶ 0007. “Where there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of

ordinary skill has good reason to pursue the known options within his or her technical grasp.”

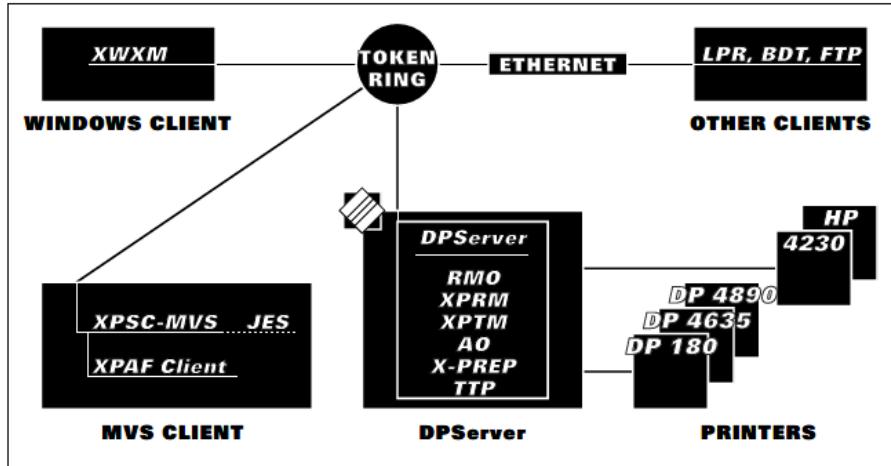
KSR, 550 U.S. at 421. Combining Caffary with Sabbagh would have yielded a predictable result, as, again, they both concern the same technical field and Sabbagh provided in detail in 2001, and thus it was known in 2007, how to augment or supplement an existing print driver. As the simple substitution of one component for another would have yielded a predictable result, one skilled in the art would have had reasonable expectation of success. “[W]hen a patent claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result.” *Id.* at 416; *Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1331 (Fed. Cir. 2009).

Therefore, Claim 4 would have been obvious to a person of ordinary skill in as early as 2003 when both Caffary and Sabbagh were available in published forms.

ii. DPServer and Caffary

DocuPrintServer Solutions Guide is a Xerox document that was published in March of 1999. (Alquist Decl. Ex. G (“DPServer”); SOF ¶¶ 18, 19.) As DPServer and Caffary were both published in this country more than one year prior to March 12, 2007, the date of application for the ’772 Patent, they are prior art to Claim 4 of the ’772 Patent under pre-AIA Section 102(b). (SOF ¶¶ 20, 13.) DPServer in view of Caffary renders Claim 4 obvious, as a person of ordinary skill would have been motivated to combine the two references with a reasonable expectation of success, which then would disclose each and every element of Claim 4.

DPServer discloses a suite of client and server resident software, including Accounting Option module (“AO”) for collection of print accounting information. DPServer at i. DPServer describes that its suite of software is used in network environments, which contains various clients, server, and printers as shown below.



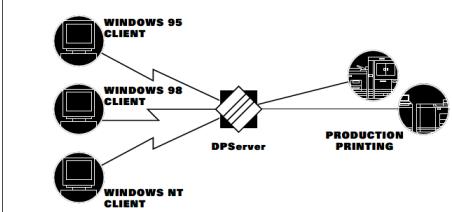
Id. at 3.

DPServer discloses that the Accounting Option module supplements XPTM, which is the driver software stored in the print server. “DPServer for the IBM RS/6000 is the server software responsible for accepting print jobs from multiple clients, passing jobs to XPTM for conversion, and scheduling the resulting PostScript or PCL job to the appropriate logical printer queue.” *Id.* at 58. The Accounting Option module tracks and locally stores document, user, and device metrics as it “records statistics and events about a client, server, and printer (if channel-attached) as related to a print job. Once a job has completed printing, the accounting information is stored in a database on the local DPServer.” *Id.* at 40-41 (emphases added). DPServer additionally discloses that the stored accounting information “may be exported (FTP) to the remote client by the DPServer operator.” *Id.* After the print usage information is saved and transferred to central data store, “[t]he information may then be analyzed using tools ranging from spreadsheets and SQL databases to accounting and data visualization packages.” *Id.* DPServer, thus, discloses every element of Claim 4 of the '772 Patent, except encryption of the captured information. However, Caffary discloses encrypting print usage information as discussed above. Caffary ¶ 0066 (“Periodically, the Client PC Software moves this temporary file in an encrypted file in the

Client PC Software installation directory named during the installation of the software.”).

Therefore, DPServer and Caffary in combination disclose each and every element of Claim 4 of the '772 Patent, as summarized in the chart below:

Claim 4 of the '772 Patent	DPServer by Xerox	Caffary (U.S. Patent Application Publication No. 2005/0259289)
<p>4. A method for managing network printers in a network including a print server having at least one existing print driver, a plurality of client terminals, and at least one printer, comprising the steps of:</p>	<p>DPServer discloses a method for managing network printers in a network including a print server having at least one existing print driver, a plurality of client terminals, and at least one printer. “The DocuPrintServer (DPServer) is a suite of client- and server-resident software modules designed to enable production printing and management in network environments for a variety of client platforms.” DPServer at i.</p> <p>In particular, DPServer includes the Accounting Option module (“AO”) that collects print accounting information for network printers connected to a plurality of client terminals.</p> <p>DPServer at 3.</p>	<p>Caffary discloses a method for managing network printers in a network including a print server having at least one existing print driver, a plurality of client terminals, and at least one printer. “The Client PC Software installs temporary software device drivers in the Windows printing sub-system on the PCS. These device drivers duplicate the function of the default Windows device drivers and are invisible to the Client PCs 60-1 . . . n, but in addition, track and record all print job related data, each time a print job is printed on a client PC 60-1 . . . n to a locally attached printer, or a server-attached printer, or to remote network printers communicating either by TCP/IP protocol or IPX/SPX protocol.” Caffary ¶ 0068.</p>
<p>appending printer management agent software to the existing print driver on said print server for monitoring</p>	<p>DPServer discloses appending printer management software to the existing print driver (XPTM). “DPServer for the IBM RS/6000 is the server software responsible for accepting print jobs from multiple clients, passing jobs to XPTM for conversion, and scheduling the resulting PostScript or PCL job to the appropriate logical</p>	<p>Caffary discloses monitoring document, user and device metrics, inclusive of origination, generation, acquisition and destination metrics, to and from the printer. “The Client PC Software serves to invisibly monitor print traffic on that client and collect data for use in the assessment. Each time a print job is created on any</p>

<p>document, user and device metrics, inclusive of origination, generation, acquisition and destination metrics, to and from said at least one printer;</p>	<p>printer queue.” DPServer at 58. <i>See also</i> DPServer at 2.</p>  <p>DPServer at 16.</p>	<p>Client PC 60-1 . . . n, the Client PC Software device driver intercepts the job instantaneously and temporarily stores the data in a file on the Client PC.” Caffary ¶ 0066.</p> <p>Caffary lists the monitored information in detail, including printer name, user logon, and document name. “At least the following data is sent by the Client PC software and stored in the Assessment Database: PrinterName, MachineName, DriverName, Location, UserLogon, MachineName, DocumentName, DataType, Copies, FileSize, Submitted, PagesPrinted. In addition, the following data may be captured Orientation, Paper Size, Paper Length, Paper Width, Scale, Print Quality, Yresolution, Color, Duplex, TTOption.” Caffary ¶¶ 0071–94.</p>
<p>capturing said document, user and device metrics by said printer management agent software each time a print job is printed to said at least one printer;</p>	<p>DPServer discloses capturing the document, user, and device metrics each time a print job is printed to the printer. Its Accounting Option module records information about the client and printer as related to the document. “The Accounting Option automatically records statistics and events about a client, server, and printer (if channel-attached) as related to a print job. Once a job has completed printing, the accounting information is stored in a database on the local DPServer.” DPServer at 40-41.</p>	<p>Caffary discloses capturing the document, user, and device metrics each time a print job is printed to the printer. “Given proper installation as per the above, all print jobs pass through the secure Print Servers and all print related data for each job is captured by the Print Job Tracking Software installed on the Secure Print Servers.” Caffary ¶ 0052.</p> <p>“The Client PC Software installs temporary software device drivers in the Windows printing sub-system on the PCs. These device drivers . . . track and record all print job related data, each time a print job is printed on a client PC 60-1 . . . n to a locally attached printer, or a server-attached printer, or to remote network printers communicating either by TCP/IP protocol or IPX/SPX protocol.” Caffary ¶ 0068.</p>

storing said captured document, user and device metrics in an encrypted file locally;	DPServer discloses storing the captured document, user, and devices metrics in a secured manner. “The power and efficiency of Xerox production printing systems is partially attributable to its ability to store resources locally at the printer - resources need not be included in the data stream or print file. Maintaining a secure resource environment only requires that you control and distribute resources from your DPServer using XPRM.” DPServer at 47.	Caffary discloses storing the captured document, user, and devices metrics in an encrypted file locally. “The Client PC Software installs temporary software device drivers in the Windows printing sub-system on the PCS. These device drivers . . . track and record all print job related data The Client PC Software then encrypts this data and sends it using TCP/IP.” Caffary ¶ 0068. “Periodically, the Client PC Software moves this temporary file in an encrypted file in the Client PC Software installation directory named during the installation of the software. Encryption is essential to prevent tampering and/or unauthorized use of the data.” Caffary ¶ 0066.
periodically writing said encrypted document, user and device metrics from said local file to a central data store;	DPServer discloses periodically writing the encrypted document, user, and device metrics from the local file to a central data store. The Accounting Option module exports the recorded information to the server resident database. “For LPR and BDT clients, accounting information stored in the server resident database may be exported (FTP) to the remote client by the DPServer operator. The information may then be analyzed using tools ranging from spreadsheets and SQL databases to accounting and data visualization packages.” DPServer at 40-41. <i>See also</i> DPServer at 5.	Caffary discloses periodically writing the encrypted document, user, and device metrics from the local file to a central data store (assessment database). “The Client PC Software then transmits the encrypted data to the Assessment Database Administrative PC on a variable time schedule that varies in accordance with print activity and is intended to minimize network traffic. For instance, if there is no print activity, then the Client PC Software reporting schedule will slow down to a minimum frequency. It has been found that a range of from every 11 seconds to every 11 minutes is suitable.” Caffary ¶ 0066.
accessing said central data store and assessing said document, user and	DPServer discloses accessing the central data store and assessing the document, user, and device metrics. The recorded information may be analyzed in the server resident database. “For LPR and BDT clients,	Caffary discloses accessing the central data store and assessing the document, user, and device metrics. “The data is then accessible on a secure basis by each dealer, for billing and operational purposes” Caffary ¶ 0054.

device metrics.	accounting information stored in the server resident database may be exported (FTP) to the remote client by the DPServer operator. The information may then be analyzed using tools ranging from spreadsheets and SQL databases to accounting and data visualization packages.” DPServer at 40-41.	“Given the foregoing data collected from all the Client PCs, a user can logon to the Assessment Database PC Software and generate a variety of reports.” Caffary ¶ 0095.
-----------------	--	--

A person of ordinary skill would have been motivated to combine DPServer and Caffary, as they both concern the same technical field—tracking and indexing print attributes. Although DPServer does not explicitly disclose encryption of captured information, it provides teaching, suggesting, and motivation to maintain a secure environment. DPServer at 47. A person of ordinary skill would have been motivated to employ the common method of securing files, such as encryption as provided in Caffary. “Encryption is essential to prevent tampering and/or unauthorized use of the data.” Caffary ¶ 0066. A person of ordinary skill would have had a reasonable expectation of success, as implementing encryption in DPServer would have yielded a predictable result without change in functions. *KSR*, 550 U.S. at 421. Therefore, Claim 4 would have been obvious to a person of ordinary skill under DPServer in view of Caffary.

iii. Coons and Shenoy

U.S. Patent No. 6,832,250 issued on December 14, 2004 from an application filed on April 13, 2000. (Alquist Decl. Ex. H (“Coons”); SOF ¶ 21.) U.S. Patent Application No. 2003/0197887¹⁴ was filed on April 18, 2002 and published on October 23, 2003. (Alquist Decl. Ex. I (“Shenoy”); SOF ¶ 23.) As both references were published in this country more than one year prior to March 12, 2007, the date of application for the ’772 Patent, they are prior art to Claim 4 of the ’772 Patent under pre-AIA Section 102(b). (SOF ¶¶ 22, 24.) Claim 4 is rendered

¹⁴ Shenoy issued as U.S. Patent No. 8,681,352 on March 25, 2014.

obvious by Coons in view of Shenoy, as a person of ordinary skill would have been motivated to combine the two references with reasonable expectation of success, the result of which discloses every element of Claim 4.

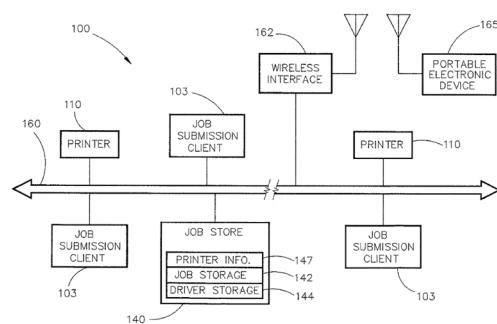
Coons concerns a system and method for remotely storing usage data associated with monitored assets. Coons Abstract. Monitored assets include printers and computers in a network setting. *Id.* col. 4 ll. 45-56. Coons discloses that its system monitors and captures usage data locally. “The usage aggregation system collects data from the monitored assets and stores this data in the local data store.” *Id.* col. 4 ll. 57-65 (emphases added). Such collection may occur at a regular interval or upon demand. “In a preferred embodiment, monitored assets are registered with the usage aggregation system. Polling of registered, monitored assets may occur on a periodic time basis. Alternatively or additionally, polling of registered, monitored assets may occur as a result of receiving a request at the local server to transmit data to the remote server.” *Id.* Coons also discloses that the usage data stored locally may be encrypted. “The local server will retrieve the usage data from the local data store 135a and, in some embodiments, encrypt the retrieved usage data prior to transmission to the remote server.” *Id.* col. 5 l. 27 - col. 6 l. 3. Further, Coons discloses that its software periodically sends the usage data to a remote server. “A local server also with access to the local data store 135a supports the transmission of the stored usage data from the local data store to a remote server.” *Id.* col. 4 ll. 29-31; *see also id.* col. 4 ll. 57-59 (“The usage aggregation system collects data from the monitored assets and stores this data in the local data store 135a. The data collection may occur in several ways. In a preferred embodiment, monitored assets are registered with the usage aggregation system. Polling of registered, monitored assets may occur on a periodic time basis.”). Coons discloses that the usage data in the local data store or the remote data store may

be subsequently accessed and assessed. “The usage data residing in either the local data store or the remote data store is available for subsequent access, processing and analysis via the local server and the remote server respectively.” *Id.* Abstract.

In summary, Coons discloses each and every element of Claim 4 of the ’772 Patent, with the exception of “appending printer management agent software to the existing print driver on said print server for monitoring document, user and device metrics, inclusive of origination, generation, acquisition and destination metrics, to and from said at least one printer.” Shenoy discloses this and several other elements of Claim 4. Shenoy concerns a system that holds output jobs, such as a document to be printed, and a plurality of print drivers. Upon demand, the system matches the output (print) job with the correct print driver based on the printer. “The printer driver storage 144 stores printer drivers corresponding to printers in the printing system 100. . . . In operation, one or more printers 110 may communicate over the network 160 (printer details are shown in FIG. 2). The job store 140 may receive a print job pull command, retrieve an appropriate printer driver from the printer driver storage 144, apply the printer driver to the print job, and supply the print job from the job storage 142 to the pulling printer.” Shenoy ¶¶ 0025–27. Specifically, Coons discloses appending an agent software (job store driver) to the existing print driver (production driver). “In the pull-based printing system according to the invention, drivers for multiple printers may be partitioned into two drivers, a job store driver and a production driver. The job store driver is used to convert a client’s print or output job into a printer-neutral format. The production driver may convert the printer-neutral print job into a format for a specific printer. The job store driver is a driver used to submit a print job to the job store 140, and is not a driver for any particular printer.” *Id.* ¶¶ 0029–30.

In addition to monitoring metrics regarding the document (output print job) and device (identity of printers), Shenoy discloses handling user specific information, such as “a user name or a job submission client identifier if the user performs an authentication process.” *Id.* ¶ 0038; *see also id.* ¶¶ 0030–31 (“The job store driver may present a user interface that enables the user to specify a finishing intent of the print job. For example, the user may specify double-sided printing, collating of the print job, stapling of the print job, etc. . . . The job store driver may include an optional interface that allows a user to specify the name of a particular printer.”) As a result, Coons and Shenoy in combination disclose each and every element of Claim 4 of the ’772 Patent, as summarized in the chart below:

Claim 4 of the ’772 Patent	Coons (U.S. Patent No. 6,832,250)	Shenoy (U.S. Patent Application Publication No. 2003/0197887)
4. A method for managing network printers in a network including a print server having at least one existing print driver, a plurality of client terminals, and at least one printer, comprising the steps of:	Coons discloses a method for managing network printers in a network including a print server having at least one existing print driver, a plurality of client terminals, and at least one printer. The usage data aggregation system monitors assets in a network, including a printer. “The local environment will typically include a communications network such as an ethernet 150 supporting communication between monitored assets such as network connected disk 141, workstation 145, printer 142, scanner 146, facsimile 143, copier (not shown), modem (not shown) and additional monitored assets and the usage data aggregation system. The local environment may further include a firewall system (not shown) and will typically include a router system (not shown). The communications network of the local environment may be connected to a larger scale communications network	Shenoy discloses a method for managing network printers in a network. “FIG. 1 is a schematic of a printing system 100 according to one embodiment of the invention. The printing system 100 may include a digital computer network 160, one or more computer output devices, such as one or more printers 110, and one or more job submission clients 103. In addition, the printing system 100 includes a job store 140 and may optionally include a wireless interface 162.” Shenoy ¶ 0017.



	such as the Internet 120.” Coons col. 41. 45-56.	
appending printer management agent software to the existing print driver on said print server for monitoring document, user and device metrics, inclusive of origination, generation, acquisition and destination metrics, to and from said at least one printer;		<p>Shenoy discloses appending printer management agent software (job store driver) to the existing print driver on said print server (production driver) for monitoring document, user and device metrics, inclusive of origination, generation, acquisition and destination metrics. The job store driver tracks document information and pull commands. “In the pull-based printing system according to the invention, drivers for multiple printers may be partitioned into two drivers, a job store driver and a production driver. The job store driver is used to convert a client’s print or output job into a printer-neutral format. The production driver may convert the printer-neutral print job into a format for a specific printer. The job store driver is a driver used to submit a print job to the job store 140, and is not a driver for any particular printer. The job store driver may present a user interface that enables the user to specify a finishing intent of the print job. For example, the user may specify double-sided printing, collating of the print job, stapling of the print job, etc. The job store driver passes these finishing intent specifications to the production driver, upon occurrence of the pull command, in order to perform the finishing of the print job by the printer.” Shenoy ¶¶ 0029–30.</p> <p>The pull commands include user metrics, such as user name. “The pull command 234 is a command or set of commands that pull print jobs from the job store 140. The pull command 234 may be a generic command that simply pulls a waiting print job.</p>

		<p>Alternatively, the pull command 234 may include information fields, such as a user name or a job submission client identifier if the user performs an authentication process.” Shenoy ¶ 0038.</p> <p>The pull commands include printer metrics, such as printer identifier. “In another alternative, the pull command 234 may include a printer identifier that specifies the printer that is pulling the print job. The printer identifier may be automatically inserted into the pull command 234 by the printer 110, or may be inserted as part of an authentication operation.” Shenoy ¶ 0039.</p>
capturing said document, user and device metrics by said printer management agent software each time a print job is printed to said at least one printer;	Coons discloses capturing usage information. The usage aggregation system monitors the assets, including the printer and polls the usage information. “The usage aggregation system collects data from the monitored assets and stores this data in the local data store 135 a.” Coons col. 4 ll. 57-65.	Shenoy discloses capturing the document, user, and device metrics by the printer management agent software (job store driver) each time a print job is printed. “Thus, if the user wants to print, the print job may be submitted to the job store 140 using the job store driver. The print jobs submitted to the job store driver may be converted to a printer independent format, such as a PDF or XHTML format, for example.” Shenoy ¶ 0029.
storing said captured document, user and device metrics in an encrypted file locally;	Coons discloses storing the captured information in an encrypted file locally. The usage data in the local data store is encrypted. “The local server including workstation 135 and server software will transmit usage data stored in the local data store 135 a to the remote server. The local server will retrieve the usage data from the local data store 135 a and, in some embodiments, encrypt the retrieved usage data prior to transmission to the remote server. In a preferred embodiment, the local server	Shenoy discloses storing the captured document, user, and device metrics in an encrypted file locally. “The user authentication information may be submitted in a suitable encrypted form and may be stored in the job store 140 along with the submitted print job. . . . In addition, in one embodiment, the document produced by the job store driver is encrypted and remains encrypted until decrypted by the printer or output device. . . . In step 426, a printer pulls the authenticated print job and prints it. The print job

	<p>will encode the usage data from the local data store 135 a in a file using commas to delimit data elements. Other embodiments may utilize encoding formats such as an XML-based encoding, SGML-based encoding or other suitable encoding format to encode the data prior to transmission. The local server will transmit the usage data utilizing an appropriate transmission protocol such as HTTP, HTTPS (HTTP protocol over a Secure Socket Layer (SSL)), FTP, SMTP, a proprietary transmission protocol or other suitable standard.” Coons col. 5 l. 27 - col. 6 l. 3.</p>	<p>therefore may be printed in response to the user authentication information input. The print job may be pulled from the job store 140 by the authenticated printer 110 and printed. Alternatively, if the user has associated the print job with a particular printer, then the print job may be pushed to the authenticating printer, or only the authenticating printer may be allowed to pull the print job.”</p> <p>Shenoy ¶ 0054–57.</p>
<p>periodically writing said encrypted document, user and device metrics from said local file to a central data store;</p>	<p>Coons discloses periodically writing the encrypted information from the local file to a central data store (remote server). “A local server also with access to the local data store 135a supports the transmission of the stored usage data from the local data store to a remote server.” Coons col. 4 ll. 29-31.</p> <p>Such polling may occur on a periodic basis. “The usage aggregation system collects data from the monitored assets and stores this data in the local data store 135a. The data collection may occur in several ways. In a preferred embodiment, monitored assets are registered with the usage aggregation system. Polling of registered, monitored assets may occur on a periodic time basis.” Coons, col. 4 ll. 57-59.</p>	
<p>accessing said central data store and assessing said document,</p>	<p>Coons discloses accessing the central data store and assessing the stored information. “The usage data residing in either the local data store or the remote data store is available for</p>	

user and device metrics.	subsequent access, processing and analysis via the local server and the remote server respectively.” Coons Abstract.	
--------------------------	--	--

A person of ordinary skill would have been motivated to combine Coons and Shenoy, as they both concern the same technical field—tracking and storing print attributes. Although Coons does not explicitly disclose “appending printer management agent software to the existing print driver on said print server for monitoring document, user and device metrics, inclusive of origination, generation, acquisition and destination metrics, to and from said at least one printer,” a person of ordinary skill would have been motivated to apply the job store system from Shenoy, published in 2003, to better manage a multitude of printers and other assets. With Shenoy’s method of holding a database of print drivers, Coon’s system would have been improved to aggregate usage data from a variety of printers. *See Dann v. Johnston*, 425 U.S. 219 (1976) (finding motivation to combine as applying a known technique would have yielded predictable results and resulted in improvement). A person of ordinary skill would have had a reasonable expectation of success, as taking a generic step of appending, or supplementing, print driver with additional software would have yielded a predictable result without change in functions. *KSR*, 550 U.S. at 421. Therefore, Claim 4 would have been obvious to a person of ordinary skill under Coons in view of Shenoy.

iv. Secondary Factors

In reaching the conclusion that Claim 4 of the ’772 Patent would have been obvious to a person of ordinary skill in the art as of about March 2007, Xerox has considered the four pertinent factual inquiries originally set out by the Supreme Court in *Graham v. John Deere Co.*,

383 U.S. 1, 17 (1966) and consistently applied by the Federal Circuit. *See, e.g., Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.*, 796 F.2d 443, 447 (Fed. Cir. 1986).

(1) With respect to the scope and content of the prior art, the Ferlitsch, Caffrey, Sabbagh, DPServer, Coons, and Shenoy references are representative of the prior art relevant to the '772 Patent.

(2) As to the differences between this prior art and claim 4 of the '772 Patent, there are essentially no differences.

(3) For the purposes of this motion, Xerox assumes the level of skill in the art set forth by Document Dynamics: "a person with a good working knowledge of software development; an understanding of the software mechanisms for local and network printing in office networks, and familiarity with methods for monitoring print activities in such networks. The person would likely have gained this knowledge through an undergraduate Bachelor of Science degree in Computer Science, or other technical degree incorporating computer science courseware, and three to five years of experience working in the field of software development and/or systems integration. Additional education or experience may serve as a substitute for these requirements." Weadock Report ¶ 21. (SOF ¶ 25.)

(4) Xerox is not aware of any objective evidence (e.g., commercial success, long-felt but unsolved needs, failure of others, copying, etc.) which would tend to establish the non-obviousness of Claim 4 of the '772 Patent. Indeed, Document Dynamics has not asserted that it makes any product that practices the '772 Patent.

Xerox reserves the right to rebut any secondary factors that Document Dynamics may put forth in its opposition brief to this motion. As a person of ordinary skill in the art would have been motivated to combine the above references and had a reasonable expectation of success in

March 2007, Xerox respectfully requests that the Court find Claim 4 of the '772 Patent obvious and invalid under Pre-AIA Section 103.

4. Indefiniteness under Section 112

Claim 4 of the '772 Patent is additionally invalid as indefinite under Section 112, as the specification fails to “particularly point[] out and distinctly claim[] the subject matter which the applicant regards as his invention.” 35 U.S.C. § 112(b). Indefiniteness is a question of law that may be decided in a summary judgment. *Noah Sys., Inc. v. Intuit Inc.*, 675 F.3d 1302, 1318–19. Courts examine whether a claim informs a person of ordinary skill of the invention’s scope with reasonable certainty when read in view of the specification and prosecution history. *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 909 (2014).

i. “Assessing”

Claim 4 is indefinite as it is not reasonably certain what “assessing” encompasses or what constitutes “assessing,” as is required by the last element of the claim. Claim 4, read in light of the specification and the prosecution history, fails to inform those skilled in the art the scope of the claimed step for “assessing” document, user and device metrics. Indeed, in preparation and filing of the '772 Patent, the patentee deleted language from the original '478 Patent specification related to “assessing.” (SOF ¶ 3.) Thus, there is no antecedent basis in the specification for the term “assessing,” which renders the claim indefinite. *Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1372 (Fed. Cir. 2014) (finding indefinite claims as “a shadowy framework upon which are located words lacking in precise referents in the specification”). Therefore, Claim 4 is indefinite as to the term “assessing.”

ii. **“Periodically”**

Claim 4 is indefinite as it is not reasonably certain how often the printer management agent software “periodically” writes the encrypted data. The ’772 Patent does not explain what it means to periodically write the data. There is no way to determine whether this term is intended to mean every second, every minute, once a month or only upon the whim of the user. Accordingly, this claim term is indefinite.

The ’478 Patent provided more information, but still fails to indicate any limits.

The Client PC Software then transmits the encrypted data to the Assessment Database Administrative PC on a variable time schedule that varies in accordance with print activity and is intended to minimize network traffic. For instance, if there is no print activity, then the Client PC Software reporting schedule will slow down to a minimum frequency. It has been found that a ranges of from every 11 seconds to every 11 minutes is suitable.

’478 Patent col. 8 ll. 45-53. Thus, based on the specification of the ’478 Patent, “periodically” is impermissibly vague because the term “periodically” can be stretched to have inconsistent meanings. As a result, Xerox respectfully requests that the Court find Claim 4 indefinite.

III. CONCLUSION

For the foregoing reasons, Xerox respectfully requests that the Court grant its Summary Judgment Motion and invalidate Claim 4 of the ’772 Patent.

By: /s/ Elizabeth A. Alquist
Elizabeth A. Alquist (ct15643)
Woo Sin Sean Park (ct30074)
Day Pitney LLP
242 Trumbull Street
Hartford, CT 06103-1212
Tel. (860) 275-0100
Fax (860) 275-0343
eaalquist@daypitney.com
wpark@daypitney.com

Attorneys for Defendant Xerox Corporation

CERTIFICATE OF SERVICE

I hereby certify that on March 15, 2019, a copy of the foregoing was filed electronically. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's CM/ECF System.

/s/ Elizabeth A. Alquist
Elizabeth A. Alquist (ct15643)